Exhibit 827-3

CHAPTER 10

Subscriber Data Management

An important area for mobile operators, but sometimes not very visible, is Subscriber Data Management (SDM). SDM is a term that may have different meanings in different contexts, but it is used here to describe the subscription handling for all processes related to, for example, privacy, authentication, authorization, policy control, and mobility management of end-users. Sometimes this is also referred to as User Data Management (UDM).

In mobile networks there are many functions and processes that require subscription-related information. The most obvious example of user subscription data that is used in LTE/EPC networks may be the user identity and security credentials that are required when an end-user device connects to an LTE/EPC network and performs authentication. The user identity (IMSI) and the security keys are stored in the USIM card in the device and the same information is also stored for each user in the operator's core network, in the Home Subscriber Server (HSS).

In mobile networks, however, a subscriber has many other parameters associated with the subscription. For example, subscriptions may differ in terms of what services they can access, what Quality of Service they will get, and what access technologies they can use, if they are charged in real time (pre-paid) or after usage (post paid), the charging model for the data consumed, etc.

In this chapter we will look at different areas of Subscriber Data Management and look at the functions and entities in the Evolved Packet Core that handle subscription data. First, we will give an overview of the different logical entities defined in EPC that maintain permanent subscriber data. These entities include the Home Subscriber Server (HSS) and the Subscriber Profile Repository (SPR). Some of this has been handled as part of previous chapters, e.g. on PCC and mobility, but in this chapter we will focus on the SDM aspects.

We will then also describe the User Data Convergence (UDC) framework defined in 3GPP. With UDC, databases for different subscriber data functions are consolidated while still maintaining compatibility towards other network entities that request subscription data, such as MME or SGSN. By consolidation of user data for different

EPC and 4G Packet Networks.
DOI: http://dx.doi.org/10.1016/B978-0-12-394595-2.00010-4

network functions and access types it is possible to provide a more efficient SDM infrastructure and to find new customer propositions.

In addition to entities permanently holding subscription data, there are different entities in EPC, e.g. the MME and the 3GPP AAA Server, that maintain subscriber data while there is an active PDN connection for a UE or may cache the subscriber data when the user is detached. However, these entities do not hold permanent subscriber data.

10.1 Home Subscriber Server (HSS)

The HSS can be described as the master database for a given user. It is the entity containing the subscription-related information to support the network entities handling mobility and user IP sessions. HSS also supports the entities handling circuit-switched calls.

Prior to 3GPP Release 5, the Home Location Register (HLR) was the main subscriber database for GPRS and circuit-switched (CS) services. The Authentication Center (AuC) was the database holding the security data for authentication of the subscriber and ciphering communication with the subscriber. From Release 5 onwards, however, the HLR and AuC functions in 3GPP specifications are considered a subset of HSS.

Figure 10.1 shows the interfaces towards the HSS. The HSS is accessible from an MME via the S6a interface, from an S4-SGSN via the S6d interface, and from a Gn/Gp SGSN via the Gr interface. The HSS is furthermore available from the 3GPP AAA

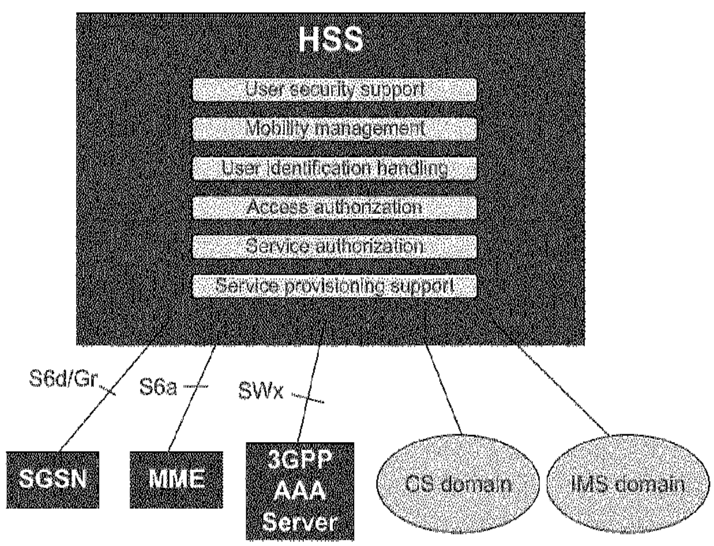

Figure 10.1: Interfaces to the HSS.
Only interfaces to EPC are shown explicitly.

Server via the SWx interface. The other interfaces to the HSS, e.g. to support the CS domain and the IMS domain, are not further described in this book, but they are the C or D interface (MAP) towards the CS domain and the Cx, Sh interfaces (Diameter) towards the IMS domain.

The S6a/S6d and SWx interfaces use the Diameter protocol and are described in more detail in Chapter 15.

The Gr interface is based on the MAP protocol and is inherited from the pre-EPC GPRS core network. Even though the EPC architecture uses S6d between S4-SGSN and HSS, the use of Gr from S4-SGSN is not precluded, e.g. for the transition from Gn/Gp SGSNs to using SGSNs supporting S4 without simultaneously needing to migrate from MAP-based HLR to Diameter-based HSS. Figure 10.2 shows a scenario where an operator has deployed S4-SGSN but kept the MAP-based Gr interface with a legacy HLR.

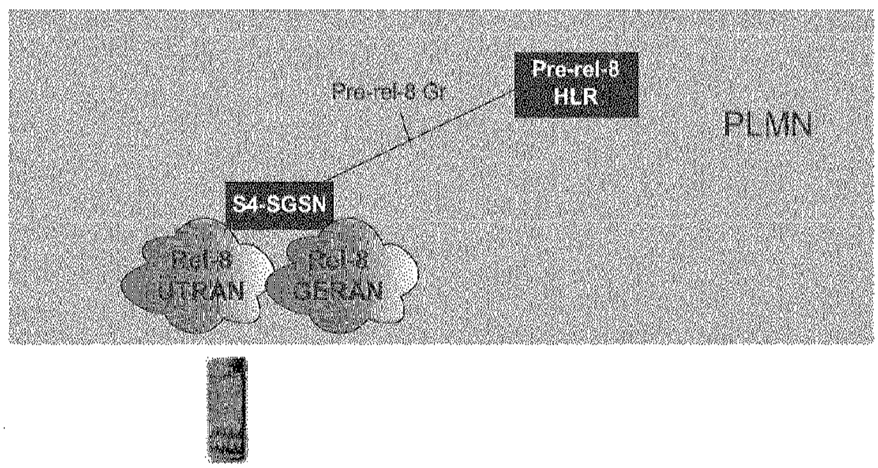

Figure 10.2: Migration Scenario with S4-SGSN and Legacy Gr/HLR.

In order to facilitate migration from HLR to HSS and to support roaming between operators with different deployments of HLR and/or HSS, 3GPP has also specified an Interworking Function (IWF) that provides protocol translation between Gr and S6a/S6d. Figure 10.3(a) shows an interworking scenario where a user from an operator with pre-Release 8 HLR is roaming in a VPLMN with EPC deployed. The IWF maps between pre-Release 8 Gr messages and S6a/Sd messages. Note that in order for this scenario to support E-UTRAN and mapping between S6a and Gr, the pre-Release 8 HLR and Gr interface must at least be enhanced to support EPS security (i.e. to deliver EPS Authentication Vectors for E-UTRAN) towards the VPLMN. Another scenario is where both operators support EPS interfaces S6a/S6d but wants to reuse the MAP/SS7 roaming infrastructure. Figure 10.3(b) shows an example scenario of such use of the IWF.

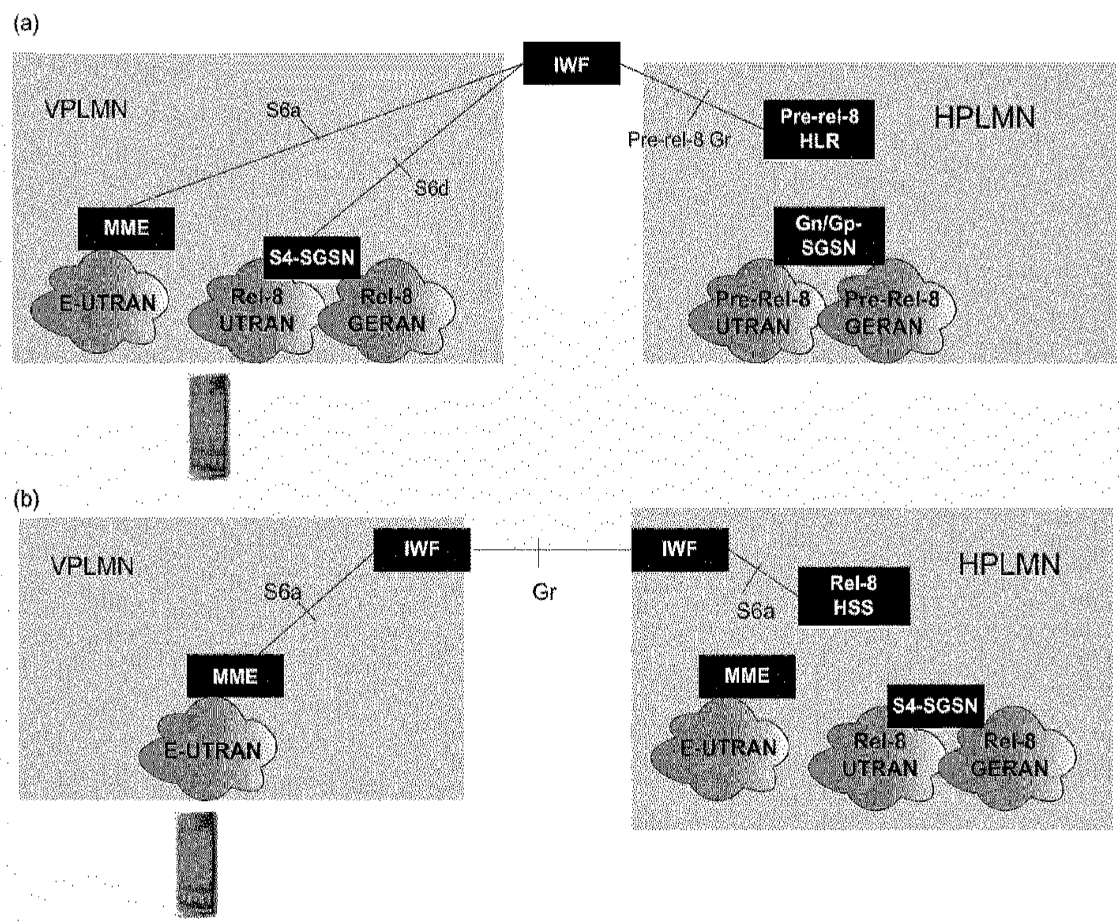

Figure 10.3: Example Interworking Scenarios Using IWF.
(a) Interworking scenario between EPC operator and operator with pre-Release 8 HLR. (b) Scenario with EPC operators roaming using MAP/SS7 roaming infrastructure.

One additional aspect when using legacy Gr and HLR with S4-SGSN and/or MME is that pre Release 8 Gr supports only delivery of GPRS subscription data. The receiving S4-SGSN and MME must therefore map the GPRS subscription data into EPS subscription data for use in EPS. How this mapping is done is not specified by 3GPP but is left to implementation and operator configuration. There are, however, a few limitations due to using pre-Release 8 Gr (either via IWF or direct) instead of using S6a/S6d. The legacy Gr interface, for example, does not support features available in the EPS subscription profile such as subscribed AMBR, dual-stack IPv4v6 bearers, handover to/from non-3GPP accesses, etc. In Release 8, Gr has, however, been enhanced to also carry the EPS subscription profile and, with such support in Gr/HLR, mapping of subscription data in MME/SGSN would not be needed.

The interested reader can consult 3GPP TS 29.305 for additional interworking scenarios using one IWF between operators with different levels of support for Gr and S6a/S6d or using two IWFs.

Even though not directly related to the topic of this section, it can also be mentioned that the IWF also supports mapping between the S13/S13′ and Gf interfaces, for equipment identity verification. See Chapter 15 for more information on the S13/S13′ interfaces.

The subscriber data and functionality of the HSS are used for a large number of functions in 3GPP networks. In the list below, we describe some of these functionalities at a high level. Many of these HSS functions are naturally reflected in other chapters of this book, where the system level functionality is described (e.g. security and mobility). Also, the functionalities of the S6a/S6d and SWx interfaces are described in Chapter 15. However, in the list below we focus on the functionality of the HSS entity as such. The functionality of HSS includes (also illustrated in Figure 10.1):

- User security support. The HSS supports authentication and security procedures for network access by providing credentials and keys towards network entities such as SGSN, MME, and 3GPP AAA Server. This aspect has been described in Chapter 7.
- Mobility management. The HSS supports user mobility by, for example, storing information about what SGSN/MME is currently serving the user. In similar ways, the HSS also supports the circuit-switched domain and IMS domain with mobility management functionality.
- User identification handling. The HSS provides the appropriate relations among all the identifiers uniquely determining the user in the system: CS domain, PS domain, and IMS (e.g. IMSI and MSISDNs for CS domain; IMSI and MSISDNs for PS domain; private identity and public identities for IMS).
- Access authorization. The HSS authorizes the user for mobile access when requested by the MSC/VLR (for CS access) and by the SGSN, MME, or 3GPP AAA Server (for PS access), by checking that the user is allowed to roam to a particular visited network.
- Service authorization support. The HSS provides basic authorization for mobile terminated call/session establishment and service invocation.
- Service provision support. The HSS provides access to the service profile data for use within the CS domain, PS domain, and/or IMS. For the PS domain, the HSS provides the APN profiles that include what APNs the user is authorized to use. The HSS also communicates with IMS entities to support Application Services.

An operator may need to have more than one HSS if the number of subscribers is too large to be handled by a single HSS. In order to support user identity to HSS resolution in such a case, Diameter agents can be deployed. The Diameter agent will

relay, proxy, or redirect the request to the appropriate HSS handling the specific user (see the Diameter protocol description in Chapter 16 for more information on the different types of Diameter agents). The Diameter agent used for user identity to HSS resolution has many similarities with the Diameter Routing Agent (DRA) defined for Diameter interfaces to the PCRF (see Chapter 9 for more details on the DRA).

Table 10.1 shows a subset of the subscriber data related to EPC access that is contained in the HSS for each given subscriber (note that the list is not exhaustive). The HSS also contains other types of subscriber data, e.g. for IMS. Readers interested in subscriber data management for IMS may consult a book dedicated to IMS, e.g. Camarillo and Garcia-Martin (2008).

10.2 Subscriber Profile Repository (SPR)

The Subscriber Profile Repository (SPR) is the database that was originally defined to hold subscription data for the PCC framework. (Later, as we will see below, an option to use User Data Convergence for PCC was also introduced.) Compared to the HSS, the SPR stores the more dynamic business rules that are needed for PCC, while the HSS contains the more static subscription data needed for network access. The reference point between the PCRF and the SPR is called Sp (see Figure 10.4). The SPR may be a standalone database but is also in many cases integrated with the PCRF.

The SPR and the Sp reference point have not been standardized in detail by 3GPP. A reason for this is that the subscription-related information that is needed by the PCRF to perform policy control is very much dependent on the services that the operator provides to its end-users. Since the type of services provided and related policies are tightly coupled to the operator business model and business offering, it is quite difficult to standardize this information. Therefore, the descriptions of the SPR and the Sp interface have been purposely left rather vague by 3GPP. Note also that there is a key difference between the S6a/S6d interfaces with HSS and the Sp interface. The interfaces S6a/S6d between the MME/SGSN and the HSS may be a roaming interface between two operators where standardization is very important, while the interface between the PCRF and the SPR is always internal to an operator.

Nevertheless, it is possible to describe at a high level what type of information may be supported by SPR. For example, the SPR may provide the following subscription profile information:

- Subscriber's allowed services
- Information on subscriber's allowed QoS
- Subscriber's charging-related information (e.g. location information relevant for charging)

Table 10.1: Subset of the Subscription Data Contained in HSS for EPC Access

Field	Description
IMSI	IMSI is the main reference key
MSISDN	The basic MSISDN (i.e. telephone number) of the UE
IMEI/IMEISV	International Mobile Equipment Identity - Software Version Number (IMEI-SV) is the identity of the actual used terminal. This is provided to HSS when the UE attaches to the NW
MME Identity	The identity of the MME currently serving this MS
Access Restriction	Indicates the access restriction subscription information, i.e. what access (e.g. GERAN, UTRAN, E-UTRAN) is not allowed
EPS Subscribed Charging Characteristics	The charging characteristics for the MS, e.g. normal, pre-paid, flat rate, and/or hot billing subscription
Subscribed-UE-AMBR	The Maximum Aggregated uplink and downlink MBRs to be shared across all non-GBR bearers according to the subscription of the user
Each subscription profile contains one or more APN profiles:	
APN Profile	
PDN Address	Indicates subscribed IP address(es)
PDN Type	Indicates the subscribed PDN Type (IPv4, IPv6, IPv4v6)
Access Point Name (APN)	A label according to DNS naming conventions describing the access point to the packet data network (or a wildcard)
SIPTO Permissions	Indicates whether the traffic associated with this APN is allowed or prohibited for SIPTO
LIPA Permissions	Indicates whether the PDN can be accessed via Local IP Access Possible values are: LIPA-prohibited, LIPA-only, and LIPA-conditional
EPS Subscribed QoS Profile	The bearer level QoS parameter values for that APN's default bearer (QCI and ARP)
Subscribed-APN-AMBR	The maximum aggregated uplink and downlink MBRs to be shared across all non-GBR bearers, which are established for this APN
VPLMN Address Allowed	Specifies whether for this APN the UE is allowed to use the PDN GW in the domain of the HPLMN only, or additionally the PDN GW in the domain of the VPLMN
PDN GW Identity	The identity of the PDN GW used for this APN. The PDN GW identity may be either an FQDN or an IP address. The PDN GW identity refers to a specific PDN GW
PDN GW Allocation Type	Indicates whether the PDN GW is statically allocated or dynamically selected by other nodes. A statically allocated PDN GW is not changed during PDN GW selection

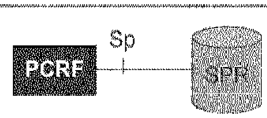

Figure 10.4: Sp Interface.

- Subscriber category
- Subscriber's usage monitoring-related information
- Multimedia Priority Service (MPS) EPS Priority and MPS Priority Level
- Subscriber's profile configuration indicating whether application detection and control should be enabled
- Spending limits profile
- A list of Application Service Providers and their applications per sponsor identity.

For more information on PCC concepts such as usage monitoring, application detection and control, and spending limits, see Chapter 8.

10.3 User Data Convergence (UDC)

In a 3GPP network, data relating to the subscriber may be managed by different network entities such as HLR/HSS and SPR. Furthermore, as we saw in the description about HSS above, there may be more than one HSS where each HSS stores subscription data for a subset of the subscribers. In that case there is a need for a Diameter agent to find the HSS that was handling a particular user.

Managing this set of databases for different kinds of subscriber data is complex and results in operational and management challenges. For example, introduction of a new user or modification of an existing subscription requires updates to multiple databases. There may also be issues with data duplication and synchronization between different locations. To resolve some of these issues, 3GPP introduced in Release 9 a new solution for User Data Convergence (UDC).

UDC aims to provide convergence of user data in order to enable smoother management and deployment of new services and networks. As we will see in more detail below, the UDC concept supports a layered architecture, keeping the actual data separate from the application logic in the 3GPP system. It does so by storing user data in a logically unique user data repository and allowing access to this data from EPC and service layer entities.

UDC aims to provide a number of benefits:

- Simplification of overall network topology and interfaces
- A single point of provision of subscriber data
- Overcoming the data capacity bottleneck of a single entry point
- Separate scaling of processing resources and data storage
- Avoidance of data duplication and inconsistency
- Avoidance of data fragmentation
- Reduction of CAPEX and OPEX for the operator.

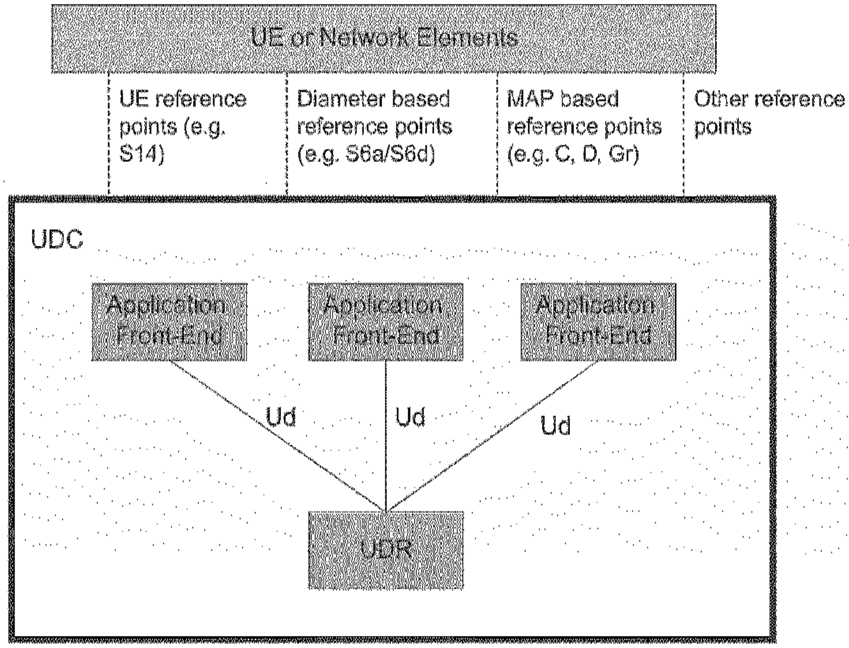

Figure 10.5: Schematic UDC Architecture.

10.3.1 UDC Overall Description

Figure 10.5 shows the logical representation of the layered architecture that separates the user data from the application logic. The user data is stored in a logically unique repository called the User Data Repository (UDR). Entities that do not store user data but need to access user data are called Application Front-Ends (FE). These Front-Ends implement the application logic for handling and operating on the user data, but they do not permanently store any user data. Examples of Front-Ends are the HSS, ANDSF, and PCRF. Access to the user data in UDR is enabled through the Ud interface.

Figure 10.6 compares a network with UDC deployed with a network where UDC is not deployed. In the non-UDC case, the network elements may have their own database storing persistent user data or they may access an external database. In the case where UDC is applied, the persistent user data is moved to the UDR. The network elements that previously stored subscription data or accessed dedicated external databases now become Application Front-Ends.

One very important aspect of UDC is that it does not affect the existing network interfaces between network entities. This can also be seen in Figure 10.6. The difference in the UDC architecture is only that a network element, which in its original form had both application logic and persistent data storage (e.g. HSS), will become an Application FE maintaining existing interfaces to other network entities, while the persistent data storage is moved to the UDR.

10.3.2 Front-Ends and User Data Repository

When the UDC architecture is applied, functional entities that originally maintained subscriber data (e.g. HSS) maintain the application logic, but they do not locally store user data permanently. As already mentioned above, these data-less functional entities become Application Front-Ends. 3GPP currently defines the following Application Front-Ends:

- HSS (and HLR/AuC)
- ANDSF
- PCRF
- IMS Application Server (AS).

The UDC also defines so-called Provisioning Front-Ends (see also Figure 10.6). These entities are used for provision of the UDR. A Provisioning Front-End provides means to create, delete, modify, and retrieve user data.

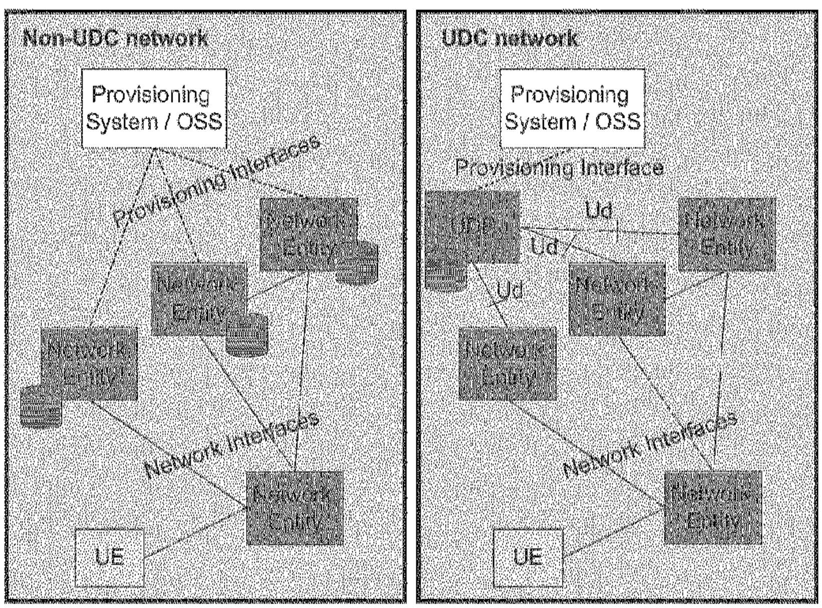

Figure 10.6: Comparison of Networks with and Without UDC.

The User Data Repository (UDR) is a functional entity that acts as a single logical repository that stores user data. The user-related data that in a non-UDC network is stored into different logical databases such as the HSS, SPR, etc. is now stored in the UDR. UDR facilitates the share and the provision of user-related data throughout services of the 3GPP system.

The UDR provides a unique reference point to one or more Applications Front-Ends. The UDR stores both permanent and more dynamic subscriber data. Permanent

subscriber data relates, for example, to the necessary information the system ought to know to perform the service. User identities (e.g. MSISDN, IMSI), service data (e.g. service profile in IMS), and authentication data are examples of subscription data. This kind of user data has a lifetime as long as the user is permitted to use the service and may be modified by administrative means. The UDR also stores temporary subscriber data. This is data that may be changed as a result of normal operation of the system or traffic conditions. Examples of temporary data are the SGSN address, user status, etc.